国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 06 月 28 日-2021 年 07 月 04 日　　2021 年第 26 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 608 个，其中高危漏洞 107 个、中危漏洞 444 个、低危漏洞 57 个。漏洞平均分值为 5.35。本周收录的漏洞中，涉及 0day 漏洞 436 个（占 72%），其中互联网上出现“WordPress 插件 Smart Slider 'name'跨站脚本漏洞、Ice Hrm 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3505 个，与上周（3577 个）环比减少 2%。

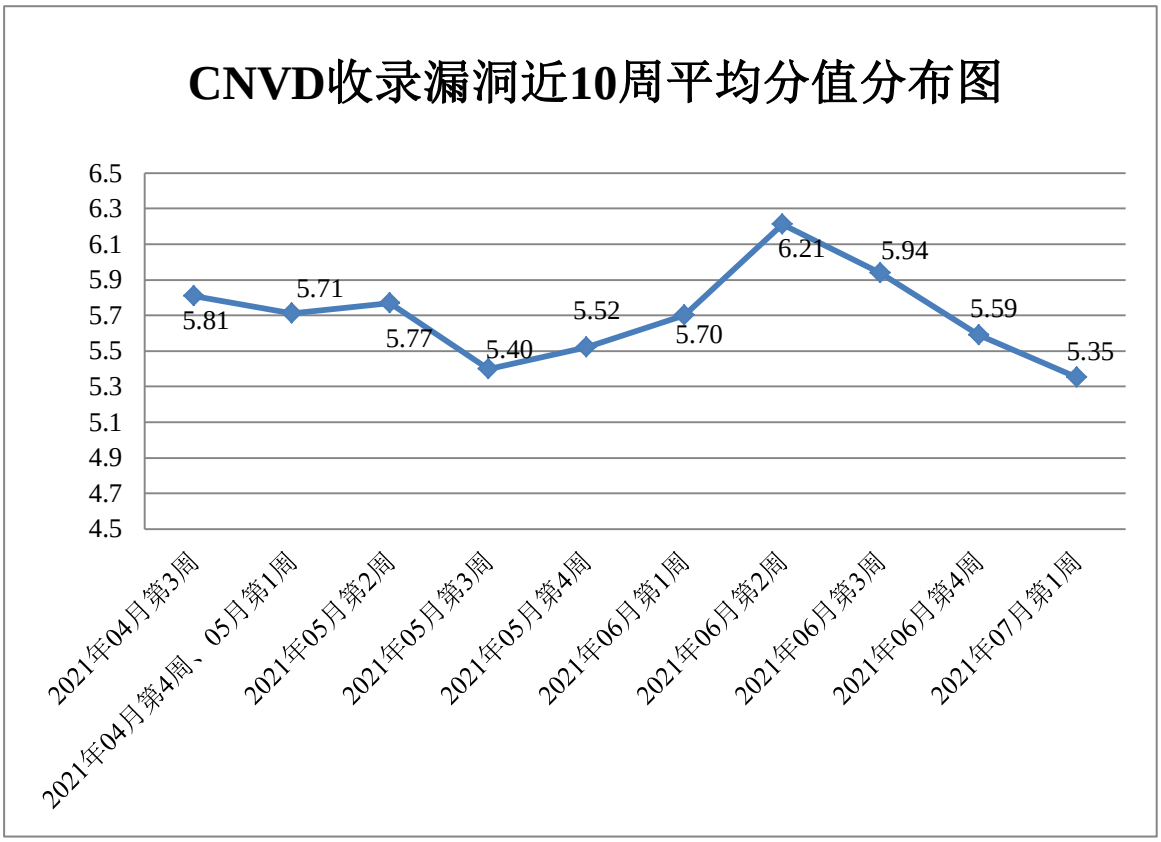

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 26 起，向基础电信企业通报漏洞事件 13 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 375 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 40 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 39 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

珠海全志科技股份有限公司、珠海金山办公软件有限公司、重庆软狐信息技术有限公司、中国电信集团公司、郑州微厦计算机科技有限公司、浙江大华技术股份有限公司、兄弟（中国）商业有限公司、夏普商贸（中国）有限公司、西安紫云羚网络科技有限责任公司、武汉烟岚科技有限公司、武汉海蜘蛛网络科技有限公司、武汉斗鱼网络科技有限公司、无锡城安信息科技有限公司、微软（中国）有限公司、苏州汉明科技有限公司、苏州恩斯特网络科技有限公司、四创科技有限公司、深圳市万网博通科技有限公司、深圳市同为数码科技股份有限公司、深圳市锟锆科技有限公司、深圳市捷顺科技实业股份有限公司、深圳市和为顺网络技术有限公司、深圳奥联信息安全技术有限公司、上海泛微网络科技股份有限公司、上海安达通信息安全技术股份有限公司、厦门四信通信科技有限公司、厦门凤凰创壹软件有限公司、三星（中国）投资有限公司、南京华智达网络技术有限公司、迈普通信技术股份有限公司、理光（中国）投资有限公司、廊坊市极致网络科技有限公司、飓风（深圳）软件有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、桂林崇胜网络科技有限公司、广州恒企教育科技有限公司、广州楚才信息科技有限公司、东芝（中国）有限公司、戴尔（中国）有限公司、北京卓正志远软件有限公司、北京中成科信科技发展有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京数科网维技术有限责任公司、北京金盘鹏图软件技术有限公司、北京棣南新宇科技有限公司、北京辰信领创信息技术有限公司、北京百卓网络技术有限公司、安徽旭帆信息科技有限公司、爱普生（中国）有限公司、京瓷株式会社、为因软件、若依、成都零起飞网络、YMBCMS、YCCMS、SEACMS、Portainer、Paessler AG、NoneCMS、Lexmark、HongCMS、Guojiz、CLTPHP、BlueCMS、Axis Communications、AKCMS、5UCMS 和 115cms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天

科技集团股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、山东新潮信息技术有限公司、新疆海狼科技有限公司、广州易东信息安全技术有限公司、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、河南灵创电子科技有限公司、安徽长泰信息安全服务有限公司、河南信安世纪科技有限公司、中国电信股份有限公司网络安全产品运营中心、北京天地和兴科技有限公司、杭州木链物联网科技有限公司、北方实验室（沈阳）股份有限公司、江西省掌控者信息安全技术有限公司、北京安帝科技有限公司、上海纽盾科技股份有限公司、北京墨云科技有限公司、武汉明嘉信信息安全检测评估有限公司、百度在线网络技术有限公司（百度 AIoT 安全团队）、南京树安信息技术有限公司、杭州天谷信息科技有限公司、长春嘉诚信息技术股份有限公司、浙江大学控制科学与工程学院、北京机沃科技有限公司、重庆贝特计算机系统工程有限公司、广州掌动智能科技有限公司、北京中科微澜科技有限公司、中油国际管道公司、中移（杭州）信息技术有限公司、浙江御安信息技术有限公司、广州安亿信软件科技有限公司、深圳市魔方安全科技有限公司、中国工商银行、海南神州希望网路有限公司、北京华云安信息技术有限公司、北京圣博润高新技术股份有限公司及其他个人白帽子向 CNVD 提交了 3505 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 1878 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
斗象科技（漏洞盒子）	864	864
上海交大	521	521
奇安信网神（补天平台）	493	493
北京天融信网络安全技术有限公司	238	7
哈尔滨安天科技集团股份有限公司	219	0
北京神州绿盟科技有限公司	175	9
新华三技术有限公司	161	0
恒安嘉新（北京）科技股份公司	122	0
北京数字观星科技有限公司	120	0

深信服科技股份有限公司	91	3
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	59	0
华为技术有限公司	59	0
北京启明星辰信息安全技术有限公司	47	0
远江盛邦（北京）网络安全科技股份有限公司	18	18
北京安信天行科技有限公司	14	14
卫士通信息产业股份有限公司	5	0
西安四叶草信息技术有限公司	4	4
北京知道创宇信息技术股份有限公司	2	0
山东云天安全技术有限公司	185	185
山东新潮信息技术有限公司	178	178
新疆海狼科技有限公司	121	121
广州易东信息安全技术有限公司	40	40
北京信联科汇科技有限公司	36	36
北京山石网科信息技术有限公司	36	36
河南灵创电子科技有限公司	28	28
安徽长泰信息安全服	26	26

务有限公司		
河南信安世纪科技有限公司	24	24
中国电信股份有限公司网络安全产品运营中心	21	1
北京天地和兴科技有限公司	17	17
杭州迪普科技股份有限公司	15	0
杭州木链物联网科技有限公司	13	13
北方实验室（沈阳）股份有限公司	12	12
江西省掌控者信息安全技术有限公司	12	12
北京安帝科技有限公司	11	11
上海纽盾科技股份有限公司	8	8
北京墨云科技有限公司	8	8
武汉明嘉信信息安全检测评估有限公司	7	7
百度在线网络技术有限公司（百度 AIoT 安全团队）	5	5
南京树安信息技术有限公司	5	5
杭州天谷信息科技有限公司	4	4
长春嘉诚信息技术股份有限公司	3	3
浙江大学控制科学与工程学院	3	3

北京机沃科技有限公司	3	3
重庆贝特计算机系统工程有限公司	2	2
广州掌动智能科技有限公司	2	2
北京中科微澜科技有限公司	2	2
中油国际管道公司	2	2
中移（杭州）信息技术有限公司	1	1
浙江御安信息技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
中国工商银行	1	1
海南神州希望网路有限公司	1	1
北京华云安信息技术有限公司	1	1
北京圣博润高新技术股份有限公司	1	1
CNCERT 山西分中心	13	13
CNCERT 天津分中心	7	7
CNCERT 青海分中心	3	3
CNCERT 上海分中心	3	3
CNCERT 海南分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 内蒙古分中心	2	2
CNCERT 西藏分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 四川分中心	1	1

个人	734	734
报送总计	4819	3505

本周漏洞按类型和厂商统计

本周，CNVD 收录了 608 个漏洞。WEB 应用 236 个，智能设备（物联网终端设备）152 个，应用程序 116 个，网络设备（交换机、路由器等网络端设备）64 个，操作系统 23 个，安全产品 17 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	236
智能设备（物联网终端设备）	152
应用程序	116
网络设备（交换机、路由器等网络端设备）	64
操作系统	23
安全产品	17

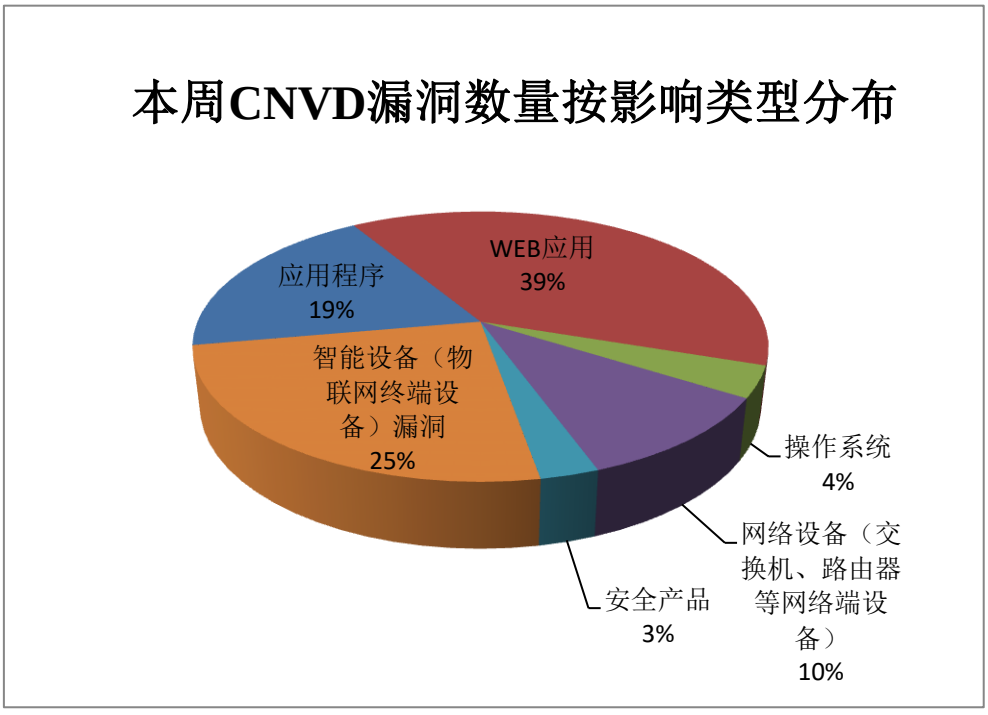

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及三星（中国）投资有限公司、Axis Communications AB、富士施乐（中国）有限公司等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例

1	三星（中国）投资有限公司	50	8%
2	Axis Communications AB	29	5%
3	富士施乐（中国）有限公司	25	4%
4	Google	25	4%
5	NETGEAR	24	4%
6	Adobe	19	3%
7	松下电器（中国）有限公司	15	2%
8	IBM	12	2%
9	成都零起飞网络	10	2%
10	其他	399	66%

本周行业漏洞收录情况

本周，CNVD 收录了 42 个电信行业漏洞，28 个移动互联网行业漏洞，23 个工控行业漏洞（如下图所示）。其中，“Google Android 越界写入漏洞（CNVD-2021-45726）、Schneider Electric PowerLogic 输入验证错误漏洞（CNVD-2021-46280）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

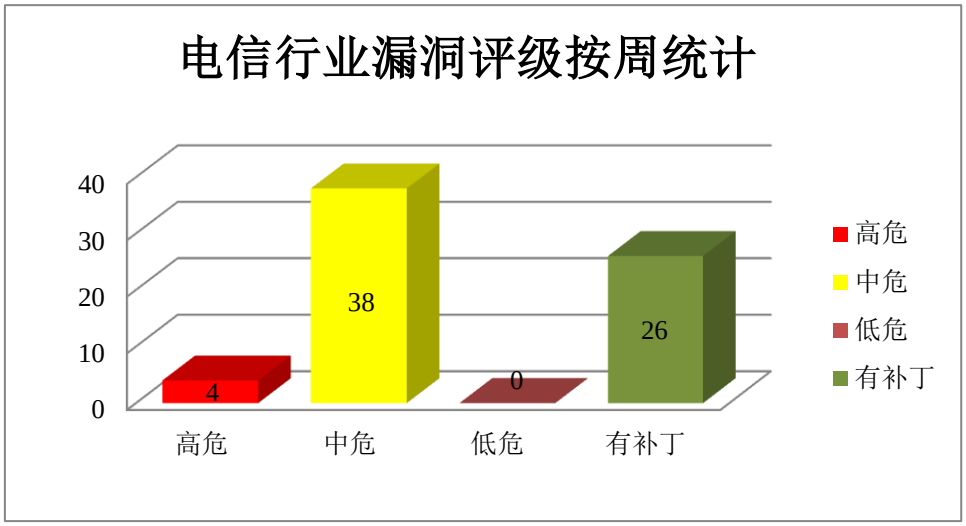

图 3 电信行业漏洞统计

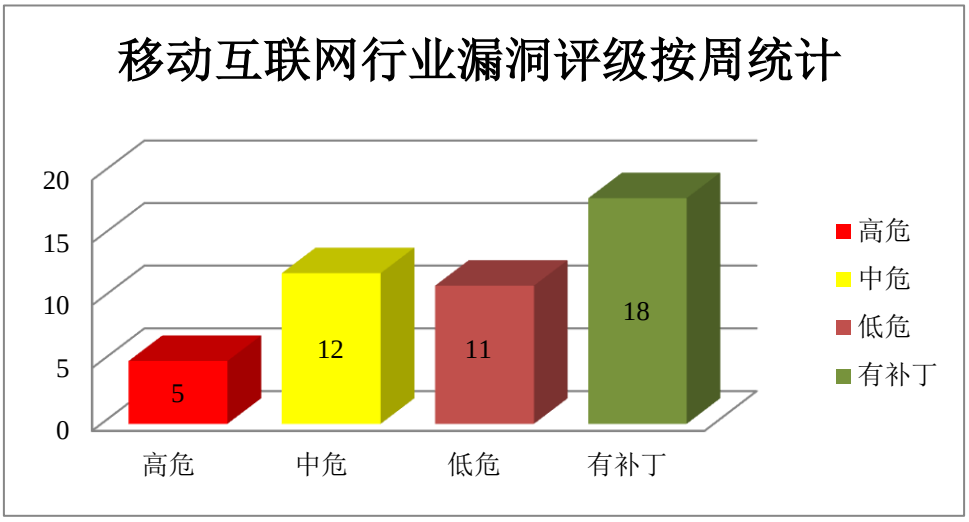

图 4 移动互联网行业漏洞统计

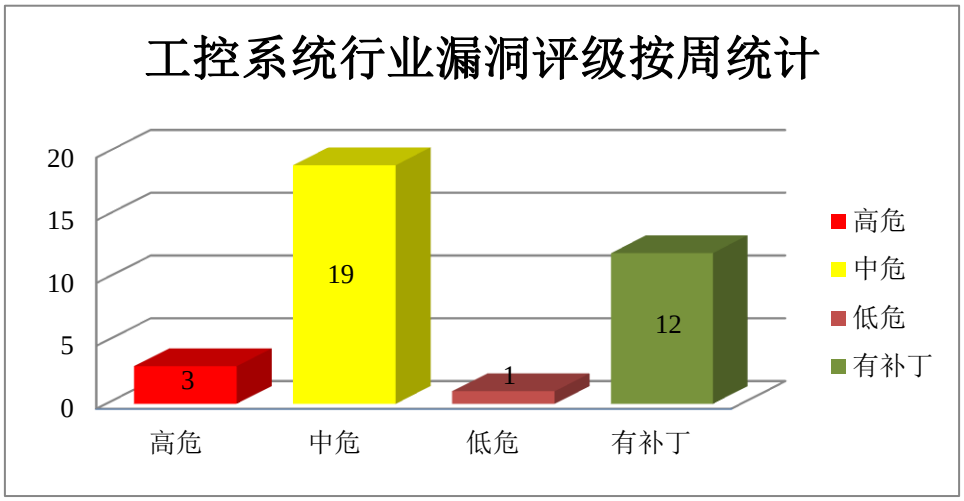

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Google 产品安全漏洞

Google Android 是美国谷歌开放手持设备联盟（Google）的一套以 Linux 为基础的开源操作系统。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升，在系统上执行任意代码或造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Google Android DevicePolicyManagerService.java 权限提升漏洞、Google Android 权限提升漏洞（CNVD-2021-45723、CNVD-2021-45729、CNVD-2021-45832、CNVD-2021-45831）、Google Chrome BFCache 代码执行漏洞、Google Chrome 扩展策略执行不足漏洞（CNVD-2021-45837）、Google Chrome 堆缓冲区溢

出漏洞（CNVD-2021-45835）。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-45439

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45723

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45729

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45730

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45832

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45831

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45837

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45835

2、Adobe 产品安全漏洞

Adobe Reader（也被称为 Acrobat Reader）是 Adobe 公司开发的一款 PDF 文件阅读软件。Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。Adobe RoboHelp Server 是面向 FrameMaker 和 RoboHelp 企业用户的基于服务器的应用程序。Adobe Animate 是一款多媒体创作和计算机动画程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 释放后重用漏洞（CNVD-2021-45945、CNVD-2021-45944、CNVD-2021-45943）、Adobe Photoshop 堆缓冲区溢出漏洞（CNVD-2021-45948）、Adobe Acrobat/Reader 越界读取漏洞（CNVD-2021-45947、CNVD-2021-45946）、Adobe RoboHelp Server 路径遍历漏洞、Adobe Animate 越界写入漏洞（CNVD-2021-45961）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-45945

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45944

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45943

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45948

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45947

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45946

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45955

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45961

3、NETGEAR 产品安全漏洞

NETGEAR D7800 是一款无线调制解调器。NETGEAR WNDR3700 是一款无线路由器。NETGEAR R6100 是一款无线路由器。NETGEAR R9000 等都是美国网件（NE

TGEAR）公司的一款无线路由器。NETGEAR EX2700 是一款无线网络信号扩展器。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-46356、CNVD-2021-46355、CNVD-2021-46354、CNVD-2021-46358、CNVD-2021-46357、CNVD-2021-46560、CNVD-2021-46563、CNVD-2021-46562）。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-46356
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46355
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46354
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46358
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46357
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46560
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46563
https://www.cnvd.org.cn/flaw/show/CNVD-2021-46562

4、Schneider Electric 产品安全漏洞

Schneider Electric homeLYnk 和 spaceLYnk 都是法国施耐德电气（Schneider Electric）公司用于不同逻辑控制器的自动化编程软件。Schneider Electric PowerLogic 是法国施耐德电气（Schneider Electric）公司的一个工控设备。提供提高功率因数来提高电源质量，排除电源故障，从而保护网络、装置和操作员。Schneider Electric Modicon M340 是法国施耐德电气（Schneider Electric）公司的一款用于工业过程和基础设施的中程 PLC（可编程逻辑控制器）。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未授权访问系统，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Schneider Electric homeLYnk 和 spaceLYnk 加密签名漏洞（CNVD-2021-45718、CNVD-2021-45720）、Schneider Electric homeLYnk 和 spaceLYnk 路径遍历漏洞、Schneider Electric HomeLYnk 和 SpaceLYnk 信息泄露漏洞、Schneider Electric homeLYnk 和 spaceLYnk 未授权访问漏洞、Schneider Electric PowerLogic 输入验证错误漏洞（CNVD-2021-46281、CNVD-2021-46280）、Schneider Electric Modicon M340 代码问题漏洞。其中，“Schneider Electric PowerLogic 输入验证错误漏洞（CNVD-2021-46281、CNVD-2021-46280）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-45718
https://www.cnvd.org.cn/flaw/show/CNVD-2021-45717

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45722

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45721

https://www.cnvd.org.cn/flaw/show/CNVD-2021-45720

https://www.cnvd.org.cn/flaw/show/CNVD-2021-46281

https://www.cnvd.org.cn/flaw/show/CNVD-2021-46280

https://www.cnvd.org.cn/flaw/show/CNVD-2021-46283

5、IBM Spectrum Protect Plus 拒绝服务漏洞

IBM Spectrum Protect Plus 是美国 IBM 公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。本周，IBM Spectrum Protect Plus 被披露存在拒绝服务漏洞。该漏洞是由于本地用户不安全的文件权限设置，攻击者可利用漏洞导致拒绝服务。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-46268

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2021-45739	Synology DiskStation Manager 释放后重用漏洞（CNVD-2021-45739）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/advisory/Synology_SA_20_26
CNVD-2021-45751	Shopware 未授权访问漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.shopware.com/en/
CNVD-2021-45942	Adobe After Effects 不受控制搜索路径元素漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/after_effects/apsb21-33.html。
CNVD-2021-46549	IBOS 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://gitee.com/ibos/IBOS/issues/I18IIV
CNVD-2021-46558	Dell PowerEdge Server 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/kbdoc/000187958
CNVD-2021-45740	Synology DiskStation Manager 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/

			advisory/Synology_SA_20_26
CNVD-2021-45948	Adobe Photoshop 堆缓冲区溢出漏洞（CNVD-2021-45948）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/photoshop/apsb21-38.html
CNVD-2021-45747	Shopware 信息泄露漏洞（CNVD-2021-45747）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.shopware.com/en/
CNVD-2021-46546	Fidelis Network Deception SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://support.fidelissecurity.com/hc/en-us/categories/360001842694-Advisories-News-and-Policies
CNVD-2021-46550	jfinal 逻辑缺陷漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/jfinal/jfinal/blob/master/src/main/java/com/jfinal/plugin/redis/serializer/JdkSerializer.java

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升，在系统上执行任意代码或造成拒绝服务情况等。此外，Adobe、NETGEAR、Schneider Electric 等多款产品被披露存在多个漏洞，攻击者可利用漏洞未授权访问系统，执行任意代码，发起拒绝服务攻击，导致缓冲区溢出或堆溢出等。另外，IBM Spectrum Protect Plus 被披露存在拒绝服务漏洞。攻击者可利用漏洞导致拒绝服务。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、WordPress 插件 Smart Slider 'name'跨站脚本漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress 插件 Smart Slider 'name'存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49958

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-46866

信息提供者

深信服科技股份有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 微软发现 Netgear 路由器漏洞导致企业被攻击

网络安全研究人员详细说明了影响 NETGEAR DGN2200v1 系列路由器的关键安全漏洞，攻击者可以利用微软在某些 NETGEAR 路由器型号中的关键固件漏洞，在企业网络中横向移动。

参考链接：https://thehackernews.com/2021/06/microsoft-discloses-critical-bugs.html

2. PowerISO 的 DMG 处理程序中存在内存损坏漏洞

TALOS-2021-1308 (CVE-2021-21871) 是 PowerISO 中的一个内存损坏漏洞，可能导致攻击者获得在受害机器上执行代码的能力。

参考链接：https://blog.talosintelligence.com/2021/06/vulnerability-spotlight-memory-.html?&web_view=true

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537